Klausur Schwerpunkt 2ms 18. April 08 Gub

---

① RSA usw.

Der öffentliche Schlüssel bestehe aus den beiden Zahlen 667 und 37.

a) Da wir es hier mit kleinen Zahlen zu tun haben, können Sie leicht die beiden Primfaktoren p und q sowie den privaten Schlüssel e bestimmen!

b) Verschlüsseln Sie die Botschaft 'J', die für Ja steht und die mit der Zeichennummer 74 codiert ist, mit dem obgenannten öffentlichen Schlüsselpaar.

c) Entschlüsseln Sie eine Botschaft, die ebenfalls nur aus ~~einer~~ einer Zahl besteht: [redacted] 19.
Das Ergebnis bedeutet die Anzahl Panini-Bildli, die ich schon besitze ...

② Das Beispiel ① zeigt (auch wenn Sie die Aufgabe nicht gelöst haben) ganz gut, worauf die Sicherheit der Methode beruht. Beschreiben Sie das in zwei, drei Sätzen.

③ IP_{18} ist die multiplikative Untergruppe aller Elemente von $\mathbb{Z}_{18}$, die ein multiplikatives Inverses besitzen.

a) Zählen Sie die Elemente von IP_{18} auf.

b) Stellen Sie die Gruppentafel auf.

c) D_3, die Symmetriegruppe eines gleichseitigen Dreiecks, hat auch 6 Elemente wie IP_{18}. Warum sind die beiden Gruppen aber sicher nicht isomorph?

① a) $p \cdot q = 667$!

factor (667) liefert sofort $p = 23$, $q = 29$ 4

→ $m = (p-1) \cdot (q-1) = 22 \cdot 28 = 616$

Der private Schlüssel ist das Inverse von 37 modulo 616 !

→ euklidin (37, 22*28) liefert $e = 333$ 4

16/16

b) Zu berechnen : $74^{37} \bmod 667$!

TR : mod (74 ^ 37, 667) = 111 ! 4

c) Zu berechnen : $19^{333} \bmod 667$!

TR : mod (19 ^ 333, 667) = 350 ! 4

Der umständliche Weg über die verschiedenen Potenzen von 2 ist gar nicht nötig.

D.h. die ganze Aufgabe lässt sich auf 4 Zeilen unseres TR lösen :

factor (667)	23 · 29
euklidin (37, 22 * 28)	333
mod (74 ^ 37, 667)	111
mod (19 ^ 333, 667)	350

② Die Sicherheit beruht einzig darauf, dass zwar das Produkt von 2 Primzahlen mit zB. 300 Stellen leicht und schnell berechnet werden kann, die Zerlegung des Produkts in seine 2 Faktoren aber enorm viel Rechenzeit beansprucht ! (Jahrhunderte oder Jahrtausende !)

8/8

Mit der public key - Verfahren entfällt dann das riesige Problem der Verteilung der Schlüssel !

(3) a) $\mathbb{P}_{18} = \{1, 5, 7, 11, 13, 17\} = \mathbb{Z}_{18}^*$ 4

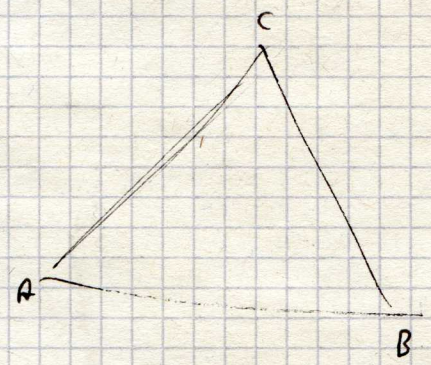
$= \{ z \in \mathbb{Z}_{18} \mid ggT(z, 18) = 1 \}$

b)

	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

10

c) D_3 ist nicht kommutativ !!



$1 = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$

$3 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$

$3^2 = 3^{-1} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$

$m_c = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$

$m_a = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$

$m_b = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$

8

22/22

$3 \cdot m_a = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = m_c$

$m_c \cdot 3 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = m_a$ ↯

oder: 4 Inversen! $\mathbb{P}_{18}$ hat nur 2

0


52
48
44
40
36
32
28
24
20
16
12
8
4
0
— 6.0
— 5.0
— 4.0
— 3.0
— 2.0
— 1.0
Ø sida > 5 ...